

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF VIRGINIA
HARRISONBURG DIVISION

IN THE MATTER OF THE SEARCH OF

**FACEBOOK USER ID:
100041314500630**

Case No. 5:20mj00015

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Robinson N. Blake, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application by the United States of America for a warrant to search and seize evidence associated with **FACEBOOK USER ID 100041314500630**, as further described in Attachment A. I am aware that information associated with a certain Facebook User ID is stored at premises owned, maintained, controlled, or operated by Facebook Inc. (“Facebook”), a social networking company headquartered in Menlo Park, California. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Facebook to disclose to the government records and other information in its possession, pertaining to the subscribers or customers associated with the above-listed User ID.

2. I am a “federal law enforcement officer” within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been since March of 2009. I am

currently assigned to the Richmond Division of the FBI, Charlottesville Resident Agency. My principal duties include the investigation of various criminal violations, to include violent criminal gangs, illegal narcotics, and interstate communication of threats. In the course of my career with the FBI, I have been involved in the execution of numerous federal search warrants, including those for social media platforms.

3. I am familiar with the facts and circumstances of the investigation through my personal participation; from discussions with other agents of the FBI and other law enforcement agencies; from my discussions with witnesses involved in the investigation; and from my review of records and reports relating to the investigation. Unless otherwise noted, wherever in this affidavit I assert that a statement was made, the information was provided by another FBI agent, law enforcement officer, or witness who may have had either direct or hearsay knowledge of that statement, and to whom I or others have spoken or whose reports I have read and reviewed. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses.

4. I am aware that Title 18, United States Code 875 (Interstate Communications), makes it a crime for anyone to transmit in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another. I am further aware that 18 U.S.C. § 2261A(2) (Cyberstalking), makes it a crime for anyone, with the intent to kill, injure, harass, intimidate, or place under surveillance with intent to kill, injure, harass, or intimidate another person, to use the mail, any interactive computer service or electronic communication service or electronic system of interstate commerce, or any other facility of interstate or foreign commerce, to engage in a course of conduct that places a person in reasonable fear of the death of or the serious bodily injury to a person or causes, attempts to cause, or would

be reasonably expected to cause substantial emotional distress to a person described in clause (i), (ii), or (iii) of paragraph (1)(A) of 18 U.S.C. § 2261A(1)(A).

5. Based upon my training and experience and the facts as set forth in this affidavit, I submit there is probable cause to believe that violations of Title 18, United States Code 875 (Interstate Communications) and/or 18 U.S.C. § 2261A(2) (Cyberstalking), have been committed by BRAXTON LOUIS DANLEY. I submit there is also probable cause to search the information described in Attachment A for evidence of these crimes, as described in Attachment B.

6. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are necessary to search the business records maintained by Facebook.

INFORMATION ABOUT FACEBOOK

7. Facebook owns and operates a free-access social networking website of the same name that can be accessed at <http://www.facebook.com>. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

8. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers (for password retrieval), physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

9. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a “Friend Request.” If the recipient of a “Friend Request” accepts the request, then the two users will become “Friends” for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user’s account includes a list of that user’s “Friends” and a “News Feed,” which highlights information about the user’s “Friends,” such as profile changes, upcoming events, and birthdays.

10. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create “lists” of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

11. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post “status” updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming “events,” such as social occasions, by listing the event’s time, location, host, and guest list. In addition, Facebook users can “check in” to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user’s profile page also includes a “Wall,” which is a space where the user and his or

her “Friends” can post messages, attachments, and links that will typically be visible to anyone who can view the user’s profile.

12. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when the user uploaded the photo or video. It also provides users the ability to “tag” (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook’s purposes, the photos and videos associated with a user’s account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

13. Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to e-mail messages, are sent to the recipient’s “Inbox” on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a Chat feature that allows users to send and receive instant messages through Facebook. These chat communications are stored in the chat history for the account. Facebook also has a Video Calling feature, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

14. If a Facebook user does not want to interact with another user on Facebook, the first user can “block” the second user from seeing his or her account.

15. Facebook has a “like” feature that allows users to give positive feedback or connect to particular pages. Facebook users can “like” Facebook posts or updates, as well as webpages or

content on third-party (*i.e.*, non-Facebook) websites. Facebook users can also become “fans” of particular Facebook pages.

16. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

17. Each Facebook account has an activity log, which is a list of the user’s posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as “liking” a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user’s Facebook page.

18. Facebook Notes is a blogging feature available to Facebook users, and it enables users to write and post notes or personal web logs (“blogs”), or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger.

19. The Facebook Gifts feature allows users to send virtual “gifts” to their friends that appear as icons on the recipient’s profile page. Gifts cost money to purchase, and a personalized message can be attached to each gift. Facebook users can also send each other “pokes,” which are free and simply result in a notification to the recipient that he or she has been “poked” by the sender.

20. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

21. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications (“apps”) on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user’s access or use of that application may appear on the user’s profile page.

22. Facebook uses the term “Neoprint” to describe an expanded view of a given user profile. The “Neoprint” for a given user can include the following information from the user’s profile: profile contact information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends’ Facebook user identification numbers; groups and networks of which the user is a member, including the groups’ Facebook group identification numbers; future and past event postings; rejected “Friend” requests; comments; gifts; pokes; tags; and information about the user’s access and use of Facebook applications.

23. Facebook also retains Internet Protocol (“IP”) logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user’s IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

24. Social networking providers like Facebook typically retain additional information about their users’ accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider’s support services, as well as records of any actions taken by the provider or user as a result of the communications.

25. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user’s “Neoprint,” IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to “tag” their location in posts and Facebook “friends” to locate each other. This geographic and timeline information may tend to either inculcate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner’s state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or

consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

26. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

PROBABLE CAUSE

27. The Federal Bureau of Investigation (FBI) is conducting an investigation into possible violations of federal criminal law committed by BRAXTON LOUIS DANLEY (“DANLEY”). On January 22, 2020, the FBI became aware that DANLEY had communicated an explicit threat against a uniformed member of the United States Army (“VICTIM”).

28. On or about January 23, 2020, I interviewed VICTIM. VICTIM informed me that VICTIM is an enlisted soldier in the United States Army (“Army”) assigned to a recruiting station in the Commonwealth of Virginia. In February of 2018, VICTIM was first contacted via e-mail by DANLEY, who expressed interest in joining the Army. In March of 2018, DANLEY went to the recruiting station to take a required entrance examination. According to VICTIM, DANLEY was unable to obtain a passing score on this test. DANLEY was instructed to continue studying in order to increase his score on the test in the future.

29. The VICTIM informed me that, in April of 2018, DANLEY called VICTIM multiple times on VICTIM’s Army issued cellular phone and general telephone number at the recruiting station, inquiring about re-taking the PiCAT. On each occasion, VICTIM or another recruiter would ask DANLEY if he had been studying for the test in order to increase his score,

and on each occasion, DANLEY replied in the negative. DANLEY was told until he studied he would not be permitted to re-take the examination.

30. On May 14, 2018, DANLEY, using e-mail address braxtonlouisdanley@gmail.com, sent an e-mail to VICTIM's official Army e-mail address that stated, "I remember every thing you pricks done to me so time to settle the score".

31. On May 14, 2018, DANLEY called the recruiting station and spoke with another identified recruiter at the recruiting station. DANLEY told the recruiter that the Army needed to arrest him (DANLEY), because he (DANLEY) was angry. On the same day, VICTIM contacted local law enforcement and filed a report regarding DANLEY's actions. Local law enforcement officers recommended VICTIM have a trespass notice sent to DANLEY.

32. On May 18, 2018, VICTIM signed a trespass notice instructing DANLEY not to trespass upon the Army recruiting station property or he would be subject to penalty of up to a \$2,500 fine and up to one year in jail.

33. On May 24, 2018, DANLEY, using e-mail address braxtonlouisdanley@gmail.com, sent an e-mail to VICTIM's official Army e-mail address that stated "Got my name and weight wrong . ." Attached to the e-mail DANLEY sent a digital photograph of the trespass notice signed on May 18, 2018.

34. On June 1, 2018, DANLEY sent a text message to VICTIM's official Army cell phone that stated "So that's how it is now you fuck my goddamn record up. Now I can't get a job anywhere ok you wanna play". On the same day, DANLEY sent another text message that stated "Yes or no need a damn answer". After these text messages, VICTIM was issued a new official Army cellular phone.

35. On July 10, 2018, between 8:59 PM and 10:09 PM, DANLEY sent, among others, the following Facebook Messenger messages to VICTIM using the Facebook account of an identified family member:

- a. “Hey it brax cant under stand why you fucked me over in that test guess cause i look like a drugy right ? . Or maybe what happened to us in high school ? . I can forget and for give but you are childish you and that fucking pope wanna fight you got one bitch ? Cant let go of the past can you . I try to fix my life and you fucked it now im hunted by your people fuck you none of you will walk away .if you wanna serve papers on me learn how to spell my name and yours . Dumb ass . Find me if you wanna fix it . To day you earn your combat pass prove it pog . Not to mention i gave my info into a fake you . A fight is here now face me”
- b. “Congrats now im fighting druggies to . Blood for blood i guess .what do you know right . Btw i have a criminal record congrat Haha now you gonna get fucked”
- c. “But works of all i though you had my back i trusted you . And you betrayed me . Fuck i would have had your back . Peace don’t know what happens now but more fights till they kill me”

36. On August 30, 2018, VICTIM was granted a Personal Protection Order (PPO) against DANLEY by the Harrisonburg/Rockingham General District Court. The PPO was served on DANLEY on September 6, 2018.

37. On December 23, 2018, DANLEY posted a message on Facebook directed at VICTIM and two other identified Army recruiters that, in part, read “your lieing fucked up my life . lock and load fuckers ima at your doorstep now .”

38. On or about January 1, 2019, DANLEY was arrested on misdemeanor charges of violation of a protective order. On or about February 26, 2019, DANLEY was convicted on the misdemeanor charge and was sentenced to 12-months incarceration. DANLEY was released from incarceration on or about June 30, 2019.

39. On or about October 4, 2019, DANLEY posted a message on Facebook that read “Traitors. Meet their ends . accidents happen...”

40. On January 21, 2020, DANLEY posted on his Facebook Account the message “24 im getin locked remember j rj this is to. you im coming to get you.” Along with the message, DANLEY posted a link to a Youtube music video by rapper sKitz Kraven titled “Mr. Roger.” I have viewed this video. The music video depicts, through images and lyrics, a violent home invasion, sexual assaults, and murder of the family residing in the home.

41. VICTIM confirmed to me that “j rj” refers to the VICTIM.

42. I am aware that VICTIM was worried for VICTIM’s safety and the safety of others working at the recruiting station because of DANLEY’s threatening communications.

43. On or about January 20, 2020, DANLEY was charged in the Commonwealth of Virginia with extortion in writing, a felony, and violation of a protective order, a misdemeanor. DANLEY. The Page County Sheriff’s Office arrested DANLEY on or about January 23, 2020, and he is currently incarcerated on these charges.

44. On February 21, 2020, I received subscriber records from Facebook for the Facebook account of BRAXTON DANLEY (vanity name braxton.danley.186). According to the records, the subscriber’s **FACEBOOK USER ID 100041314500630** and the account were registered on September 6, 2019. The subscriber records also listed cellular telephone number XXX-XXX-8578 as being associated with the Facebook account.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

45. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular, 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Facebook to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

46. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Facebook who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

47. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated.

48. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

REQUEST FOR SEALING

49. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

OATH

The information in this affidavit is true to the best of my knowledge and belief.

Respectfully submitted,

s/Robinson N. Blake

Robinson N. Blake
Special Agent - FBI

Received by reliable electronic means and sworn and attested to by telephone
March
on this 31st day of ~~April~~ 2020.


— JOE C. HOPPE —
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with **FACEBOOK USER ID 100041314500630** that is stored at premises owned, maintained, controlled, or operated by Facebook Inc., a company headquartered in Menlo Park, California, for the period of February 18, 2018 to January 23, 2020.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Facebook

To the extent that the information described in Attachment A is within the possession, custody, or control of Facebook Inc. (“Facebook”), including any messages, e-mails, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for each user ID listed in Attachment A:

- (a) All contact and personal identifying information, including: full name, user identification number, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. If any of the aforementioned Facebook pages are group accounts, all of the following information is requested: group identification number, a list of users currently registered to the group, and Group Contact Info, including all contact information for the creator and/or administrator/s of the group and a PDF of the current status of the group profile page.
- (b) All activity logs for the account and all other documents showing the user’s posts and other Facebook activities;
- (c) All photos and videos uploaded by that user ID or Facebook accounts associated with the email addresses of the administrators, and all photos and videos uploaded by any user that have that user tagged in them together with any and all photos

identified by Facebook using Facebook's facial-recognition software to match the images uploaded by the user IDs;

- (d) All profile information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;
- (e) All other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, and pending "Friend" requests;
- (f) All "check ins" and other location information;
- (g) All IP logs, including all records of the IP addresses that logged into the account;
- (h) All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";
- (i) All information about the Facebook pages that the account is or was a "fan" of;
- (j) All past and present lists of friends created by the account;
- (k) All records of Facebook searches performed by the account;
- (l) All information about the user's access and use of Facebook Marketplace;
- (m) The types of service utilized by the user;

- (n) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
- (o) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;
- (p) All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. § 875 (Threats) and/or 18 U.S.C. § 2261A(2) (Cyberstalking) involving the user **FACEBOOK USER ID 100041314500630** including, for each username or display name identified on Attachment A, information pertaining to the following matters:

- a. Communications between BRAXTON LOUIS DANLEY and others related to the crime(s) under investigation;
- b. Threats or communications by BRAXTON LOUIS DANLEY to injure, intimidate, harass, or interfere with another person or to damage their reputation.
- c. Threats or communications by BRAXTON LOUIS DANLEY to extort or blackmail another person for financial gain.

- d. Communications by BRAXTON LOUIS DANLEY that could place a person in reasonable fear of death or serious bodily injury to the person, the person's immediate family member, or the person's spouse or intimate partner.
- e. Communications by BRAXTON LOUIS DANLEY that could cause or attempt to cause substantial emotional distress to another person, an immediate family member, or spouse or intimate partner.
- f. Evidence indicating how and when the Facebook account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Facebook account holder;
- g. Evidence indicating the Facebook account user's state of mind as it relates to the crime under investigation;
- h. The identity of the person(s) who created or used the username or display name, including records that help reveal the whereabouts of such person(s).

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS
RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)**

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Facebook, and my official title is _____. I am a custodian of records for Facebook. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Facebook, and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of Facebook; and
- c. such records were made by Facebook as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature